Global Information Assurance Certification Paper

Phillip M. Cox

October 8, 2002

GCWN Certification Program

Practical Assignment Version 3.1

Option 1

Design a Secure Windows 2000 Infrastructure

Introduction:

Giac Enterprises, a fictitious company that researches and sells network adapters is based in Albuquerque, New Mexico with a remote office across the city. Giac specializes in multi-speed adaptors that run on a variety of hardware and operating systems. Giac is very concerned about the security on their network. They have very valuable data that resides on the internal network that needs to be safeguarded at all times. This data includes research and development information that many of Giac's competitors would like to have. This paper will describe the steps necessary to secure Giac Enterprises active directory deployment across their internal network.

Currently Giac has four main departments. They are: Research and development, Sales and Marketing, Finance and Human Resources, and the IT department. Each department has a different mission for the success of the company and needs to be looked at differently in terms of securing the organizational unit that each department will be a part of.

Research and Development:

The Research and Development department is the hub of Giac Enterprises. This is where all of the new technology is designed and tested. This is also the department that needs to be the securest in terms of locking down data and auditing user access to make sure that the valuable data is never in the wrong person's hands. The R & D department consists of 20 scientists, 10 technologists, and 3 secretaries. This information will help determine the active directory layout for this department in the active directory design stage.

Sales and Marketing:

The Sales and Marketing department specializes in advertising and sales of the network adaptors. This department's main function is to sell the network cards. Since this department deals with sensitive information it will need to be locked down so that only the people who need to know the information, will get the information. This is necessary because there will be customer contact names, addresses and personal information.

Finance and Human Resources

Just like most companies, Giac's Finance and HR department needs to be secure because of the controlled information that this department posses and processes. This department is in charge of all the money and finances that Giac receives and sends out and it is in charge of every employees personal and salary information. This data needs to be treated as Official use only and needs to be audited when people access the data.

IT

The IT department will consist of desktop and server administrators that run the network and computer systems for Giac. The members of this group will have admin rights on a lot of machines so this group needs to be audited and secured to make sure that no one gains unauthorized access into the admin groups.

Assumptions

There are many assumptions in this paper that need to be addressed for this paper to make sense. I will cover these assumptions now so that the total layout of the design will make more sense.

- The only operating system that will be allowed is Windows 2000. This was decided on for security reasons and to make it easier on the administrators. This allows for secure authentication to the domain controllers and all desktops can take full advantage of Active Directory.
- There will be a corporate Anti-Virus server that pushes all updates to the clients. This server will be Norton Anti-Virus 7.61 and will be controlled by the corporate IT department. All desktops will be configured to have real time protection services on at all times. The corporate server will control this. All servers will be scanned nightly because of the overhead that the real time services causes on systems.
- All corporate servers and networking equipment will be stored in a vault. All access to this vault will be limited to IT personnel and will be audited weekly to see if there is any misuse of the system. Video cameras will also be installed in the vault for security reasons.
- All networking equipment and connections are already installed and configured. This includes the main T1 connection to the Internet and the dedicated T3 connection between the home office and the remote site. This connection will be hardware encrypted on both ends to make it more secure.
- The remote office is the office where the Research and Development department is located. Since this department is a Research and Development department they will need access to the Internet to get up to date data on the projects that they are working on. This will be possible by a T1 line going to the Internet.
- All servers will have the latest Service Packs and security hot fixes installed. This will be done by a product called Update Expert[1]. This allows an administrator to remotely push any released hot fixes to his servers. It will also let you install multiple hot fixes at one time by knowing the release date of the hot fix and knowing when it should be installed. This software is made by St. Bernard software.

[1] http://www.updateexpert.com

Network Design and Diagram:

In order to secure any Active Directory deployment, it is necessary to plan and diagram the network design. This allows you to see the whole picture and plan accordingly. Diagram 1 shows the geographic layout of the servers and where they are located in the enterprise.

Since security is of the utmost concern, the two offices will be connected with a dedicated T3 line. Even though this will cost more money for the corporation, it will give them added security between sites. As mentioned in the assumptions, the two sites will be encrypted with hardware encryptors on both sides.

DMZ

The DMZ will house the servers that will be seen on the Internet. The external firewall that stands between the DMZ and the Internet is configured to only allow DNS, e-mail, and http, https traffic through. This allows traffic that is needed for the mission of the corporation but drops all other traffic before getting into the company. This includes the DNS servers, the IIS servers and the external e-mail server. All servers will be Windows 2000 server with service pack 3 installed.

Since these servers are in the DMZ, they will be more vulnerable to attacks then the servers that are in the internal network. All servers will be locked down with the latest NSA security configuration guides. This includes the guide to the secure configuration and administration or Microsoft Internet Information Services 5.0, the guide to the secure configuration and administration of Microsoft Exchange 2000, and the guide to securing Microsoft Windows 2000 DNS. This will give us a base line security and then we can lock down the machines to fit our environment.

The servers that are in the DMZ will not be a part of the internal domain. In fact they will all be stand-alone machines. This is necessary to protect the internal domain from any compromise that might happen to the DMZ machines. If something happens to a machine on the DMZ then that is all that a hacker will get. They will not gain any access to any resources on the internal domain. This will help keep the classified and confidential information secure.

The following is a table of the machines in the DMZ. This describes the kind of hardware, software, and configurations that are on each machine.

Server Name	Server Type	RAID Level	Size of Disks	Memory	Processor
Dc01	Dell 6450	RAID 0+1	18 gig*2	2 gigs	Quad Pentium III 700 mhz Xeon
dc02	Dell 1550	Raid 1	18 gig*2	1 gig	Dual Pentium III 800 mhz
dc03	Dell 1550	Raid 1	18 gig*2	1 gig	Dual Pentium III 800 mhz
dc04	Dell 1550	Raid 1	18 gig *2	1 gig	Dual Pentium III 800 mhz
fs01	Dell 2650	Raid 5	18 gig*2 (OS) 36*12 (data)	2 gigs	Dual Pentium III 1 ghz
db01	Dell 6450	Raid 0+1 (OS) Raid 5 (data)	18 gig*2 (OS) 36*12 (data)	4 gigs	Quad Pentium III 700 mhz Xeon
ms01	Dell 6450	Raid 0+1 (OS) Raid 5 (data)	18 gig*2 (OS) 36*12 (data)	4 gigs	Dual Pentium III 700 mhz Xeon

Table 1

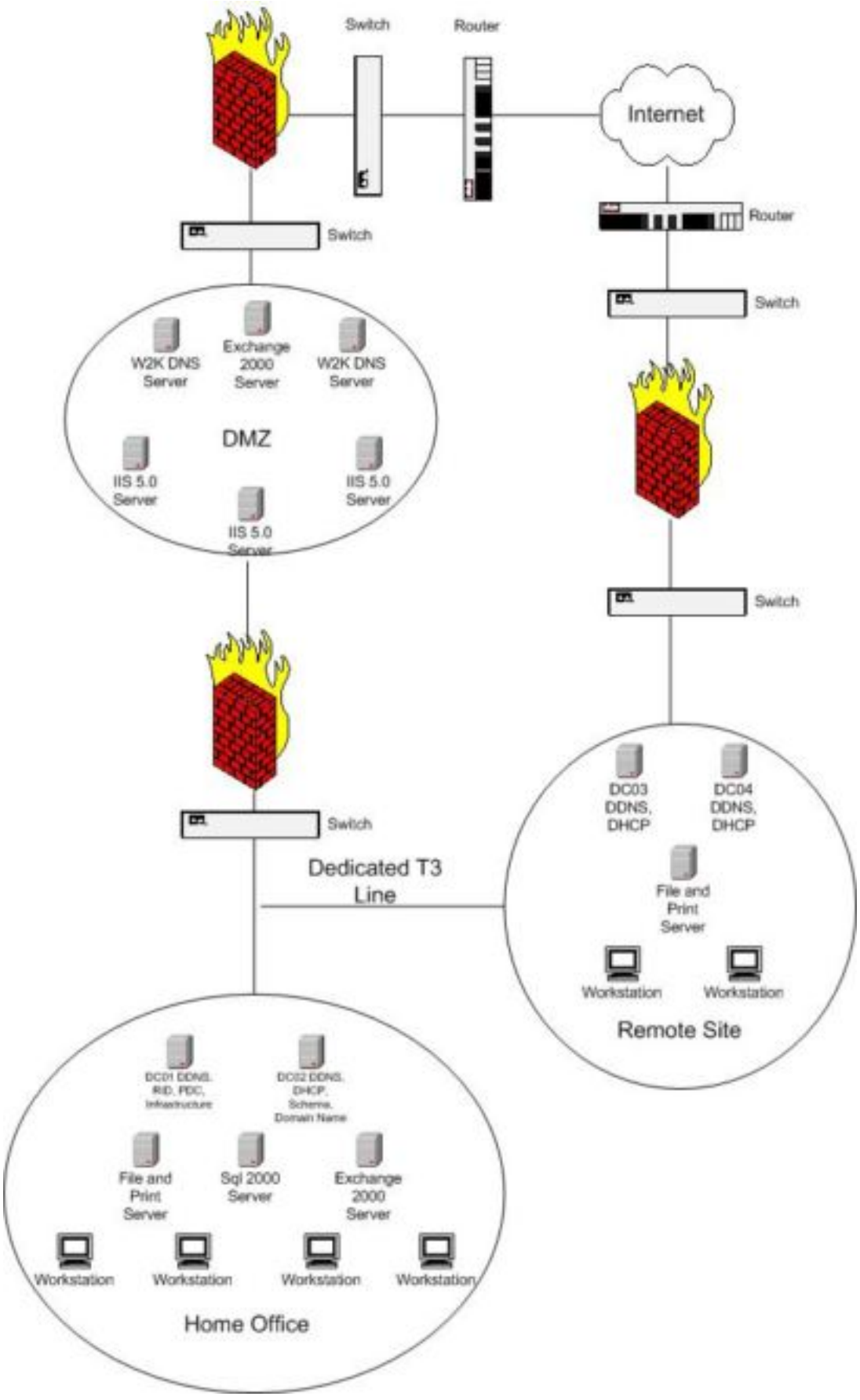

Diagram 1

Active Directory Design and Diagram:

Since Giac is a relatively small company, it makes sense to have only a single domain model, with multiple Organizational Units below the domain. The Organizational Unit structure will be based on the physical layout of the corporation. For example, the Human Resources and Finance department will have their own OU with the users, computers, and printers in their own OU's below the top level. This will allow for many Group Policy Objects depending on what type of security each department needs. Diagram 2 will show the whole layout for the active directory domain including Organizational Unit structure.

The reason why a single domain model makes sense is because of the way that Giac Enterprises is constructed. Since management wants to have all departments in different OU's, it makes sense to have one domain and control user and computers from those OU's under the domain. It also makes sense because there is less administrative overhead with the single domain model. If you only have one domain then you don't have to worry about trusts between the domains and it takes away an area that could potentially break.

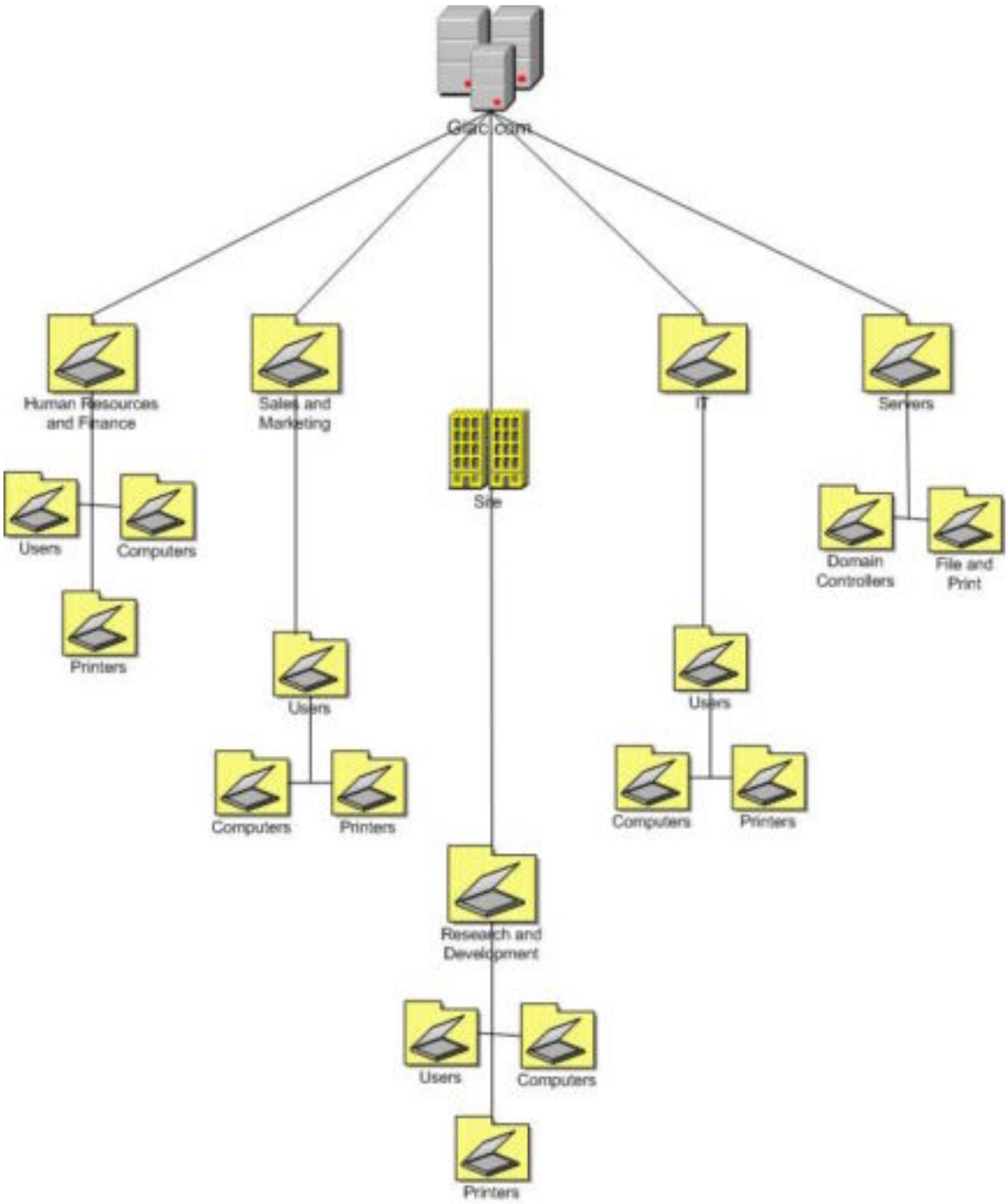

Diagram 2

Giac Domain:

The following table is of the Server hardware that is in the Intranet.

Server Name	Server Type	RAID Level	Size of Disks	Memory	Processor
dc01	Dell 6450	Raid 0+1	18 gig*2	2 gigs	Quad Pentium III 700 mhz Xeon
dc02	Dell 1550	Raid 1	18 gig*2	1 gig	Dual Pentium III 800 mhz
dc03	Dell 1550	Raid 1	18 gig*2	1 gig	Dual Pentium III 800 mhz
dc04	Dell 1550	Raid 1	18 gig *2	1 gig	Dual Pentium III 800 mhz
fs01	Dell 2650	Raid 5	18 gig*2 (OS) 36*12 (data)	2 gigs	Dual Pentium III 1 ghz
db01	Dell 6450	Raid 0+1 (OS) Raid 5 (data)	18 gig*2 (OS) 36*12 (data)	4 gigs	Quad Pentium III 700 mhz Xeon

Table 2

The Giac domain will be the only domain at the corporation. All corporate policies and business rules will be applied at this level and then replicated down to the organizational units. Since all policies are replicated down by local, site, domain and then OU, we will have to make sure that all of these policies will not be overwritten by the organizational unit's group policy when it is applied after the domain policy. The organizational unit's group policy will only contain settings that deal particularly with the department itself. This means that the domain policies are the least amount of protection that an OU must have but if an OU needs tighter restrictions then they will be set in the OU's group policy.

Since there is a home office and a remote office at Giac Enterprises we will be putting a site in Active Directory at the remote office. *In Active Directory terms, a site is one or more well-connected TCP/IP subnets organized for security and replication topology. In this definition, well connected means fast and reliable connections*.[2] Since we have a T3 between the two offices, this is no problem to do this. The reason to put a site up at the remote office is to control the amount of traffic between the two sites. With a site up we can configure how often and when replication occurs between the domain controllers at both sites. For Giac we will trigger replication every fifteen minutes. This will keep the remote domain controllers up to date but will not create a lot of traffic between the WAN links.

Inter-site replication can use one of two protocols to replicate data. They are Remote Procedure Call (RPC) and Simple Mail Transport Protocol (SMTP). Since we would have to get a certificate to secure SMTP, we will use RDP to replicate the data. By default RPC is encrypted and will be secure enough to fit our needs.

The other benefit of putting up a site at the remote office is for subnets. Since our remote office has a different subnet then our home office, this will work perfectly. Our remote office's subnet is 192.168.12 and our home office's subnet is 192.168.10. The reason this is nice is because we can put in the subnets into the site and the site will know which subnet belongs where. Then when I put in a machine with the IP Address of 192.168.12.45, it will automatically go into the remote site because I have configured the sites with IP Addresses. This will help with the administrative overhead and will make the lives of the administrators a little easier.

[2] MCSE Windows 2000 Migration Study Guide, page 241. San Francisco: Sybex, 2001.

As shown in the Network diagram, we will have two domain controllers at the home office and two domain controllers at the remote office. This will allow for fault tolerance and will reduce the loads on the domain controllers themselves. This is necessary for two reasons. If something happens to the hardware at either site on one of the domain controllers, there will be another one there. Although some of the FSMO roles will have to be transferred to the server that is running, the domain will be functional and people will still be able to authenticate to it. The other reason is for networking issues. If the T3 link between the two sites happens to go down, then the remote site will still have a domain controller with all of the information in the directory. Once the link comes back up, the domain controllers will replicate any new data that has happened since the link was down.

FSMO Roles (Flexible Single Master Operation)

Since Active Directory is a multi-master database, it has to allow changes to the database from any one Domain Controller at any one time. Since this has to happen the possibility exists that conflicts of data can lead to problems after all of the Domain Controllers have replicated to each other. To handle this problem, Windows 2000 incorporates an algorithm that says the last writer wins. This means that the last Domain Controller that updated Active Directory is the one that has the correct version of the data. On some updates this algorithm works fine but for a lot of updates Active Directory can only have one updating Domain Controller. This is where the FSMO Roles come into play. These roles are assigned to only one domain controller but each role can be on a separate domain controller. This allows Active Directory to act in a single-master fashion, allowing the one Domain Controller to update the directory with the only correct copy of the data. The following is a list of the FSMO Roles and how they are used in Active Directory.

- **Schema Master –** The schema is what the directory is all about. It tells the Active Directory database what needs to be in it. It is also completely configurable. The Schema Master writes this configuration to the database. When an administrator updates the schema it connects to the domain controller that has the Schema Master role. After the schema has been updated it then replicates to the other domain controllers. The Schema Master will reside on DC02.
- **Domain Naming Master –** The Domain Naming Master is the Domain Controller that is in charge of adding and removing a domain from the directory. Since Giac Enterprises is a single domain model, we won't be using this FSMO role but it will reside on DC02 in case Giac grows to a multiple domain model.
- **RID Master –** The RID Master is in charge of giving each Domain Controller RID's to handout while creating user's or groups in Active Directory. Each security principal that is created in Active Directory has a security identifier (SID), part of this SID is the relative identifier (RID). The other part of the SID is the same for all security principals in the domain. The unique part is the RID and it has to be different for each object. In order for each object to be unique the RID Master gives each domain controller a pool of RID's to use. This way no RID can be the same for two objects. This FSMO role will reside on DC01.

- **PDC Emulator –** In a network that has NT 4.0 and below clients, servers and domain controllers, the PDC emulator acts like a Primary Domain Controller and all directory writes must go through it. Since we have a total Windows 2000 network, the clients can contact any DC to perform a directory write. That DC will then replicate to all of the other DC's in the domain. Even though it looks like the PDC Emulator will not be utilized in our domain, it will be. In a total Windows 2000 domain, the PDC emulator is used to synchronize the time in the enterprise. This is necessary for the Kerberos authentication protocol. This keeps all machines with the same time. Since this part of Kerberos tickets is so important we will be synching this DC with the U.S. Naval Observatory timeserver every night. This FSMO role will reside on DC01.
- **Infrastructure –** The infrastructure role is used to update references across multiple domains. The Infrastructure role queries the Global Catalog server to see what changes have occurred and update their references accordingly. This role will reside on DC01, but will not be used because of our single domain model.

Organizational Units

Microsoft made huge strides to make administrators lives easier when they tied in Organization Units to Active Directory. The OU's allow you to put any object into that OU and manage it from there. You no longer have the problem of having multiple domains to match the way that your corporation is physically setup. You can now have a single domain with multiple OU's to address the different departments and geographical locations. This is the model that Giac decided to use for their Active Directory model. All of the OU's will have the same bottom level OU's below the top level. These include, Users, computers, and printers. This is true for all top-level OU's except for the Server OU. It will only house servers in their respective Organizational Unit, which is described in detail below.

The OU setup also allows for Delegation of Control. This delegation of control allows administrators to define exactly what another user can do. In the past if an administrator wanted to allow a user to add computers to a domain, they would have to give that user account operator rights. This is okay if the user knows what they are doing and can be trusted not to do anything else. Giac does not want to take this risk and has decided to delegate control to users that need certain rights to fulfill their job requirements. Now an administrator can create a group, delegate control to this group and then populate this group with the users that need to do this. In order to delegate control in Active Directory, we will do the following:

1. Open Active Directory Users and Computers.
2. Right click the object that needs delegation of control.
3. Choose Delegate Control.
4. Click next on the delegation of control wizard.
5. Choose the group that needs delegation of control.
6. In the next window choose either of the two radio buttons depending on what you want the group to be able to do. This is where you can either give them a lot of power, or you can limit them to do very little.
7. In the next window you will decide on what permissions they will need to get their job done.

8. In the last window, check all of the settings that you have made on the previous windows and then click finish.

After the delegation of control is complete we will create a test user and put him in this group to make sure that he can only do what we have allowed him to do. If he can do more then he is suppose to do, then we will need to look at why he can do more and then fix the problem.

The following is a description of all of the OU's in the Giac.com domain.

1. **Human Resources and Finance:** This OU will house all of the users, computers, and printers in the HR and Finance department. This Organizational Unit currently houses 30 user accounts, 32 computer accounts, and 10 printers. This Organizational Unit needs to be setup a little different and more secure because of the sensitive data that will reside on these machines.
2. **Sales and Marketing:** Since the users in this OU will not be processing such sensitive data, we will not have as restrictive settings on these computers. Even though the data that will be on these computers is considered official use only, it is not classified or sensitive since it is not R&D or employee salary and personal information like it is in the other departments.
3. **Research and Development:** This organizational unit will be the most restrictive in terms of locking machines down to restrict access and to protect the data. All machines will be audited daily for insider threats with a third party utility called Aelita[3]. This allows us to get a report of all event logs on specified machines and then query these logs for a specific user, time or event. This is necessary because the data on these machines will be considered classified and no one without need to know should be accessing this data.
4. **Server:** The Server OU will house all of the corporate servers in their respective bottom OU depending on the function that the server is playing. There will be a Domain Controller and File and Print server OU that will be below the top level Server OU. This will allow us to put GPO's on each OU and lock it down to that specific function that each server is playing. It will also allow us to drag and drop new machines into the respective OU and then all security and configuration settings will be applied with no extra work from the administrator.
5. **IT:** The IT OU will consist of the members of the IT department. This department needs to be watched closely and will be monitored to see who is added into the OU. The reason being is because the members in this department will have Domain Admin rights. There is currently only five members of this group which makes it very easy to audit and control permissions on this OU.

Basic Group Policy

Group Policy is where most of the security configuration is done in Windows 2000. This allows us to set policies that must be adhered to when the machine boots up or when each user logs on. Each policy will be configured to update every 30 minutes. Since Giac Enterprises is a relatively small corporation this will not be too much of a

[3] http://www.aelita.com

burden on the network or on the domain controllers themselves. This allows administrators to change the policy at any time and know that within thirty minutes all clients will have the new settings without a desktop visit. This cuts down on administrative work for the desktops.

After each of the GPO's are installed, it is necessary to run the Security Configuration and Analysis snap-in. This will analyze the computer and tell us that all of the settings that we created in the template are applied correctly. To do this, follow the following steps:

1. Open the MMC console by typing MMC at the run command.
2. Go to Console and then Add/Remove Snap-in.
3. Click on Add.
4. Choose Security Configuration and Analysis Snap-in.
5. Click close.
6. Click ok on the Add/remove snap-in box.
7. Right click Security Configuration and Analysis
8. Choose open database.
9. Name the database the same as the GPO that you are analyzing.
10. Choose the .inf file that contains your template that you have already created.
11. Click open.
12. Again right click Security Configuration and Analysis.
13. Choose Analyze Computer Now.
14. Choose a file path for the error log and say ok.
15. After analyzing, click on the plus next to Security Configuration and Analysis.
16. Go through each of the headings and see what each one says.
17. If there is a green checkmark you are good to go.
18. If there is a red X then something is wrong and further troubleshooting is required to see why the policy is not being applied.

Although this tool does not test every setting that is applied in a GPO. It does test all of the security settings that we are most concerned with. It is an easy way for auditing individual machines to see if the policy is really doing what it is suppose to be doing. In fact Giac has a policy in place that 25% of all machines will be audited this way every six months. The policy also states that a random sample of machines will be taken from all GPO's and not just one. This makes the auditors happy because they can actually see if the settings are taking place without having to go to multiple places to see what the settings are. In other words they can do it all from one nice console.

Group Policy for the Domain Controllers

The following is a description of the major security aspects in Giac's default domain controller's policy. In the auditing section most everything is turned on so that we can see who is doing what and when they are doing it. We need to be able to audit who logs on to what machines and who is trying to log on to machines. With this policy we will need to increase our security log sizes to 100 mb. Each night the third party utility will grab the event logs and put them into a sql database that then allows us to query on any string that we want. This also allows us to overwrite logs when necessary because all data is stored and backed up on the sql server.

1. **Audit Policies**
    a. **Audit Account Logon Events:** Success, Failure.
    b. **Audit Account Management**: Success, Failure.
    c. **Audit Directory Service Access**: Success, Failure.
    d. **Audit Logon Events:** Success, Failure.
    e. **Audit Object Access**: Success, Failure.
    f. **Audit Policy Change:** Success, Failure.
    g. **Audit Privilege Use**: Success, Failure.
    h. **Audit System Events:** Success, Failure.

2. **User Rights Assignment**
    a. **Access this computer from the network:** Administrators, Authenticated Users, Enterprise Domain Controllers.
    b. **Add Workstations to Domain:** Administrators. We only want admins to be allowed to add machines to the domain. This allows us to have greater control to know who is on the domain at all times.
    c. **Change the system time:** Administrators. This is necessary so that the system time does not change for Kerberos tickets.
    d. **Logon Locally**: Administrators.
    e. **Manage auditing and security log:** Administrators.
    f. **Restore Files and Directories:** Administrators. Although most people believe that backup operators should be in this group, I think that only admins should be because of the sensitive data on the domain controllers.

3. **Security Options**
    a. **Audit use of backup and restore privilege:** Enabled. This will allow us to see who is restoring what on the DC's.
    b. **Clear virtual memory pagefile when system shuts down:** Enabled. Although this makes reboots a whole lot longer, the machine is more secure if someone who should not have physical access to the machine gets physical access.
    c. **Digitally sign client communication (when possible):** Enabled.
    d. **Digitally sign server communication (always):** Enabled.
    e. **Do not display last user name in logon screen**: Enabled. Since only administrators can logon to these machines, we do not want any one seeing who is an administrator and getting the user name.
    f. **Lan Manager authentication level**: Send NTLMv2 response only\refuse LM & NTLM: This setting encrypts all logons so that it makes it harder for people sniffing the network to crack the passwords.
    g. **Rename Administrator Account:** Enabled.
    h. **Rename Guest Account**: Enabled.

4. **Event Log**
    a. **Maximun size for all logs**: 100 MB. As stated above this size will be large enough for a days amount of events.
    b. **Restrict guest access to all logs:** Enabled.

5. **Restricted Groups**
    a. We will leave this as the default.

6. **System Services**
    a. Since each domain controller does different things we have a corporate policy to change service settings on each domain controller when that domain controller is installed. This allows us to set services to different settings.

7. **Administrative Templates**
    a. **Group Policy:** The group policy refresh interval should be set to every ten minutes on domain controllers. This will make sure that all DC's are up to date with the latest GPO.

All other settings in the GPO have to do with software installations or application configurations. Since this is a default domain controllers policy, we will not be setting any of these settings here. We will have a lot of these settings in the default domain policy that will be described next. The purpose of this policy is to secure the domain controllers themselves and to make sure that all auditing is turned on, on all domain controllers. This makes all of the DC's look the same across the whole domain.

Default Domain Policy

1. **Software**
    a. This section is for installing software remotely to each computer that is in the OU. Since this is a domain GPO, it does not make since to have any software remotely installed at this level. It makes more sense to do this at a department level GPO.
2. **Windows Settings**
    a. Scripts: This section is used to apply logon and logoff scripts to users who login to the domain. Giac has a logon script that makes sure that each user has the Norton anti-virus installed and that the virus definition files are up to date. This helps us keep out viruses that have already been identified and a fix has been created for them. Currently this is the only script that is run.
3. **Security Settings**
    a. Password Policy
        i. Enforce password history: 10
        ii. Maximum Password age: 180 days
        iii. Minimum Password age: 1 day
        iv. Minimum Password Length: 8 Characters
        v. Passwords must meet complexity requirements: Disabled. Giac decided to use a complex password generator for all passwords that are created. Since this generator creates passwords that meet our complexity requirement we do not need to do it here. Users are not allowed to change their password except through the generator utility.
    b. Account Lockout Policy

i. **Account Lockout Duration:** 0
ii. **Account Lockout threshold:** 5 invalid logon attempts. This allows the user plenty of tries to get the password correct but does not give a hacker very many attempts at guessing it.
iii. **Reset Account Lockout Counter After:** 120 Minutes.

4. **Local Policies**
   a. **Audit Policy**
   Once again we need to be auditing users actions on machines across the domain for unauthorized access to data. This will be done with the following settings on auditing on every machine in the domain.
      i. **Audit account logon events:** Success, Failure.
      ii. **Audit account management:** Success, Failure.
      iii. **Audit Directory service access:** Failure.
      iv. **Audit logon events:** Success, Failure.
      v. **Audit Object Access:** Failure.
      vi. **Audit Policy Change:** Success, Failure.
      vii. **Audit Privilege use:** Failure.
      viii. **Audit process tracking:** No Auditing.
      ix. **Audit system events:** Success, Failure.
   b. **User Right Assignment**
   This section is a very extensive section covering a lot of what each user can do on every machine in the domain. This is where we will lockout unauthorized users from gaining access to machines and lockout users from doing things that only Administrators should be doing. The following is a list of the most important settings in this section.
      i. **Access this computer from the network:** Administrators, Authenticated users.
      ii. **Force shutdown from a remote system:** Administrators.
      iii. **Logon as a batch job:** Administrators.
      iv. **Logon Locally:** Administrators, Authenticated users.
      v. **Manage auditing and security log:** Administrators.
      vi. **Take ownership of files or other objects:** Administrators.
   c. **Security Options**
   In this section we will cover who can do what and where they can do it. We will also establish what kind of signatures and encryption will be used to talk with other machines and servers in the network. Again I will only be outlining the most important settings in this section.
      i. **Allow System to be shutdown without having to logon:** Disabled. This setting needs to be disabled so that only authenticated users can shutdown a machine after they have logged on.
      ii. **Clear virtual system pagefile when system shuts down:** Enabled. Gets rid of important information that is stored in the pagefile that possibly a hacker could get to or someone that has physical access to the drive.
      iii. **Disable CTRL+ALT+DEL requirement for logon:** Disabled. This setting needs to be disabled so that the logon message that Giac has will be shown before the user actually logs on.

iv. **Do not display last user name in logon screen:** Enabled. Once again this is so that someone walking by cannot just hit ctrl+alt+del and see who logged in last. This is half the battle for a hacker. If he knows the username, then he can start trying to crack the password.

v. **Message text for user attempting to logon:** Enabled
Since users have to say ok to the logon text, this is a great place to tell them that the machine they are accessing is not theirs and that anything that they do can be audited. Here is Giac's logon banner.

   a. This computer system is the property of Giac Enterprises. It is for authorized use only. User (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized Giac personnel as well as authorized officials from other agencies. By using this system, the user consists to such interception and disclosure at the discretion of Giac Enterprises. Unauthorized use of this system may result in administrative disciplinary action and civil and criminal penalties. Press the "ok" button to indicate your awareness of and agreement with the terms and conditions of this warning notice. If you do not agree with these terms and conditions DISCONTINUE all efforts to access or utilize Giac Enterprises computing equipment and information.

vi. **Prevent users from installing printer drivers:** Enabled. Drivers can be an easy way for hackers to get into a system. Only administrators should be able to do this.

vii. **Prompt user to change password:** Disabled. This is disabled because of the password generator utility e-mails a user when their password is fixing to expire.

viii. **Rename Administrator account:** Enabled. This is good practice and should be done on all machines.

ix. **Rename Guest account:** Enabled. Just like the administrator, this should be done on all machines.

x. **Restrict CD-Rom Access to locally logged-on user only:** Enabled.

xi. **Restrict Floppy access to locally logged-on user only:** Enabled. This is important because only the person at the console should be using the peripheral drives. This applies to both the cd and the floppy drives.

xii. **Shutdown system immediately if unable to log security audits:** Enabled. This is a very important indicator that something is wrong with your machine. If it shuts down because it cannot log security events it could save your machine from being hacked into. Even though this could risk data loss, I think that it is an acceptable risk to take to protect our systems.

5. **Event Log**
    a. **Settings for event logs**
    All of the other settings (not included below) in the section have to deal with log retention dates. Again since we are collecting our logs and putting them into a SQL database, none of these settings mean anything, so we are going to not include them in this discussion.
        i. **Maximum application log size:** 24960 kilobytes
        ii. **Maximum security log size:** 49984 kilobytes
        iii. **Maximum system log size:** 24960 kilobytes. On all of these log settings we have given enough space for one days collections. Since our third party util will grab the collections daily. We don't have to worry about losing logs to audit.
        iv. **Restrict Guest Access to application log:** Enabled.
        v. **Restrict Guest Access to security log:** Enabled.
        vi. **Restrict Guest Access to system log:** Enabled. We do not want to allow any guest access to any logs because a user could read or clear any log. This includes hackers.
        vii. **All of the other settings in the section have to deal with log retention dates.** Again since we are collecting our logs and putting them into a SQL database, none of these settings mean anything, so we are going to not include them in this discussion

6. **Restricted Groups**
    We will leave the default on this section.
7. **System Service**
    Since this is a domain policy it would be hard to limit services on all of the machines out there. Therefore I will not be defining anything in this section so that users don't break. This should be done at a departmental level OU where each department decides what is on each computer.
8. **User Configuration**
    a. **Software Installation:** Here again I don't think that this needs to be by user, it needs to be by machine and what ever OU that machine is in.
9. **Windows Settings**
    a. **Internet Explorer Maintenance:**
        i. **Browser user interface:** This section is where we will put in our custom logo on IE and we can customize Browser Toolbar buttons.
        ii. **Connection:** This will allow us to set the proxy settings for all browsers and all users.
        iii. **Security:** The security section allows us set security in the browser itself so that users will receive a secure browser. We will have our browsers on the medium level.
    b. **Folder Redirection:**
    Here we will redirect all users My Documents to the corporate file server. This is necessary so that all users data gets backed up nightly. We can also restore their data if something gets corrupt or if the user accidentally deletes something.
10. **Administrative Templates:**
    In this section I will only discuss the security related sections.

a. **Windows Update**
    i. **Remove access to use all windows update features:** Since we are using a third party utility to roll all patches and hotfixes that the IT department has tested and approved, I do not want the users to be able to update their own systems without the IT groups knowledge.
b. **System**
    i. **Group Policy refresh interval for users:** This will be enabled and left to the default 90 minutes setting and the random time added will be 30 minutes. This setting will update every users settings every 90 minutes. The other setting is so that every client does not access the DC's for their policy update at the same time.

Although the domain policy covers a lot of security and GPO settings we will be going over two more OU policies in detail. I will only be describing the things that are particular to that OU.

Research and Development Computers Group Policy

1) **Software:** Through this utility we will install all software to all computers in this OU. This will allow us to have a common operating environment across all computers in the R&D OU. This is necessary to have stable machines for the scientists to do their complex calculations on. It also takes the risk out of allowing users the right to add and remove programs themselves. This actual feature will be shown in a lower policy.
2) **Security Settings**
    a) **Account Policies:** These will stay the same as the domain.
    b) **Local Policies:**
        i) **Audit Policy:** The audit policy will change a little since these machines process classified data. I will only mention the ones that are changing.
            (a) Audit Object Access: Success, Failure.
            (b) Audit Privilege Use: Success, Failure.
            (c) Audit Process Tracking: Success, Failure.
        ii) **User Rights Assignment:** This will stay the same as the domain.
        iii) **Security Options:** This will stay the same as the domain.
    c) **Event Log** This will stay the same as the domain.
3) **User Configuration (Windows Settings)**
    a) **Administrative templates**
        i) **Control Panel**
            (1) Disable Add/remove Programs: Disabling this option will help the configuration of the users machines. Since they won't be able to add or remove programs, their machines will stay the same. Not only is this easier for the administrators, but it is more secure because users can't install programs that have not been tested and approved.
            (2) Disable Display in control panel: We do not want the users messing around with the display section for administrative purposes.
            (3) Password protect the screen saver: enabled. This option needs to be enabled for security reasons. Many times a user will walk away from their computer and forget to lock their workstation. Since these machines have

sensitive data on them we will be password protecting the screen saver, so that it locks in a specified amount of time.

(4) Screen Saver Timeout: 360 seconds. The amount of time for the screen saver to be locked. We decided that 360 seconds (six minutes) is about the right amount of time. We don't want to burden the users while they are still at their desk, but we want to make sure that the screen saver comes on in a reasonable timeframe.

(5) Disable addition of printers: enabled. All printers are networked printers and will be added through a log on script.

ii) System

(1) Disable Registry editing tools: enabled. No user needs access to their registry. This will not allow them to poke around and try changing settings.

(2) Run only allowed Windows Applications: enabled. This will help with only letting users run certain applications that Giac is currently licensed for.

(3) Disable Change Password: enabled. All passwords will be changed through the password change utility.

(4) Group Policy refresh interval for users: set to 90 minutes and 30 minutes for the random.

This is all of the changes that we will make on the R&D OU. This will help secure the systems but it will also make the administrators life a little easier by not letting the users play with things and break them.

The next OU that I will talk about will be the Human Resources and Finance. Since this department deals with personal and salary information, we will be locking it down to protect that information.

Human Resources and Finance Group Policy

1) **Software** We will be doing the same thing in this OU as we did in the R&D OU. We will install all software on all machines through this mechanism.
2) **Security Settings**
   a) **Account Policies:** These will stay the same as the domain.
   b) **Local Policies:**
      i) **Audit Policy:** The audit policy will change a little since these machines process sensitive data. I will only mention the ones that are changing.
         (a) Audit Object Access: Failure.
         (b) Audit Privilege Use: Failure.
         (c) Audit Process Tracking: Failure.
      ii) **User Rights Assignment:** This will stay the same as the domain.
      iii) **Security Options:** This will stay the same as the domain.
   c) **Event Log** This will stay the same as the domain.
3) **User Configuration (Windows Settings)**
   a) **Administrative templates**
      i) **Control Panel**

(1) **Disable Add/remove Programs:** Disabling this option will help the configuration of the users machines. Since they won't be able to add or remove programs, their machines will stay the same. Not only is this easier for the administrators, but it is more secure because users can't install programs that have not been tested and approved.
(2) **Disable Display in control panel:** We do not want the users messing around with the display section for administrative purposes.
(3) **Password protect the screen saver:** enabled. This option needs to be enabled for security reasons. Many times a user will walk away from their computer and forget to lock their workstation. Since these machines have sensitive data on them we will be password protecting the screen saver, so that it locks in a specified amount of time.
(4) **Screen Saver Timeout:** 360 seconds. The amount of time for the screen saver to be locked. We decided that 360 seconds (six minutes) is about the right amount of time. We don't want to burden the users while they are still at their desk, but we want to make sure that the screen saver comes on in a reasonable timeframe.
(5) **Disable addition of printers:** enabled. All printers are networked printers and will be added through a log on script.

ii) **System**
(1) **Disable Registry editing tools:** enabled. No user needs access to their registry. This will not allow them to poke around and try changing settings.
(2) **Run only allowed Windows Applications:** enabled. This will help with only letting users run certain applications that Giac is currently licensed for.
(3) **Disable Change Password:** enabled. All passwords will be changed through the password change utility.

iii) **Group Policy refresh interval for users:** set to 90 minutes and 30 minutes for the random.

Additional Security

Windows 2000 has made great strides in trying to make their operating system more secure. This is definitely evident with the Group Policy Objects. Although this helps a lot in securing a system, it is not all that you need to do. To secure Giac's network, we did the following things.

DMZ DNS Machines

The machines in the DMZ will need to have local security policies set so that they are secure to hack attempts. The following is what we will do on top of the NSA's recommendation guide to securing Windows 2000 DNS servers.

1 Account Policies

a **Password policy:** This policy needs to be very strict so that passwords are not the weakest link on these servers.

i **Maximum Password age:** 30 days. The maximum age will be thirty days on all passwords on this server.

ii **Minimum password length:** 16 characters. The length of all passwords will be sixteen characters on this server. This is necessary so that it is harder for the passwords to be cracked.

b Account Lockout:

i Account Lockout threshold: 1 invalid logon attempt. Since only the administrators should be logging into this server, we will only allow one invalid logon attempt. This will slow down the hackers who are trying to guess the usernames and passwords on this machine.

2 Local policies:

a **Audit Policy:** The audit policy will audit all events. This will allow us to see exactly what is happening on a machine. Some events will only log failures because it will not do any good to log success on these events.

i **Audit account logon events:** Success, Failure.
ii **Audit account management:** Success, Failure.
iii **Audit Logon Events:** Success, Failure.
iv **Audit Object Access:** Failure.
v **Audit Policy Change:** Success, Failure.
vi **Audit Privilege Use:** Success, Failure.
vii **Audit System Events:** Failure.

b **User Rights Assignment:** The following will describe what user can do what on these machines. Since this machine is a server, only administrators will be allowed to do anything on this machine.

i **Access this computer from the network:** Administrators.
ii **Logon locally:** Administrators.
iii **Manage auditing and security log:** Administrators.
iv **Shutdown the system:** Administrators.

c Security Options:

i We will leave the settings that NSA recommends.

d **System Services:** I will only mention the ones that I will be disabling.

i **Application Management:** Disabled. Since this service is used for software installation via a corporate network, it will not be needed on these servers.
ii **Automatic updates:** Disabled. All updates will be done through Update Expert.
iii **Clipbook:** Disabled. This service is only used to create and share data to be viewed by remote computers. It does not affect the local clipboard on the local system. Since we will not be sharing data on the clipboard with other machines, this service will be disabled.
iv **DHCP Client:** Disabled. This server will have a static IP Address and will have no need for DHCP.
v **DFS:** Disabled. This server will not need to have DFS enabled because no users will need to be on this machine to access data in the logical namespace.
vi **Distributed Transaction coordinator:** Disabled. This service keeps track of transactions that span across multiple systems. This could include databases, message queues or file systems. This service is usually used for COM+ and SQL server.
vii **Fax Service:** Disabled. No faxes should be sent to or from this machine.

viii **Internet Connection sharing:** Disabled. The DNS servers do not need to be sharing an internet connection with any client that might be out there.
ix **Intersite Messaging:** Disabled. We do not need to be sending or receiving messages from other windows server sites.
x **Netmeeting:** Disabled. This service allows users to use netmeeting, we do not want anyone using netmeeting on these machines.
xi **Print Spooler:** Disabled. There should be no printing from this machine.
xii **Remote Registry Service:** Disabled. No remote registry manipulation will be allowed. All registry manipulation will be from the console.
xiii **Routing and remote Access:** Disabled. This server does not need to be a router or a RAS server. This service needs to be disabled.
xiv **SMTP:** Disabled. This server will not need to send e-mail, so this service will be disabled.
xv **Telnet:** Disabled. We do not want anyone to be able to access this computer through telnet. Telnet is not secure and needs to be left out of this network.

Patches

The biggest problem with most machines on any network is that they are still at the same service pack as when they started. Most hackers in the world are not true hackers; they are what we call script kiddies. This means that they search the Internet looking for scripts that they can run against machines that are vulnerable. The sad thing is, is that most of the time there is a patch released for that vulnerability. If sys admins will just test and patch their machines when the patch is released, we could almost eliminate most of the hackers out there. As mentioned before, Giac uses a utility called Update Expert to push all of their patches. This utility connects into Microsoft's database for released patches and downloads them to the local machine. You can then query each machine and it will tell you what you are running and at what SP level you are at. In other words it sees what level you are at and then only gives you the hotfixes and patches for your machine. You can then click on each hotfix and it brings up Microsoft's website for that patch so that you can get more information about that particular patch. I think that this has saved us so much time and energy trying to keep patches up to date.

Physical Security

You can have all of the security in the world on the software but if you don't have physical security protecting your infrastructure servers, then all the other security does not matter. Giac has a vault that all servers are kept in, including the servers at the remote site. Access is controlled through a badge swipe, which logs all entrances and exits into the vault. There is also video recording equipment to make sure that nothing "disappears" in the night. All these measures are necessary because a hacker could get the hard drives or ERD's of the machines and get passwords. Once he has these, it is all over. The rest of Giac's machines will have power on passwords and locks on the cases so it will make getting into the machine a little harder. This will prevent people from reseting the power on password and getting into the machine.

Network

Giac has made it a policy that no wireless networking equipment will be allowed on the premises. It just is not secure enough to let their precious data get hacked into because of the convenience that wireless offers. In the future when wireless networks are more secure, Giac will look at the issue again and will make a decision at that point. This is a great policy to have but it will need to be enforced to make sure that no one in the company is breaking this rule. It is very easy for a user to put up a wireless access point in his office. With this being said it will be necessary for Giac to have a product that detects wireless networks so that we can shut them down. The product that Giac has chosen is called Isomair[4] Wireless Sentry. This product was chosen with the future of wireless in mind. With this product we can set up sensors around Giac Enterprises and centrally manage every sensor that is out there with one central server. These sensors are configured to detect any new wireless access point, no matter what it is. We can then find the wireless access point and shut it down. In the future when Giac decides to deploy wireless, this product will be the perfect tool to be using and we will not need to purchase any more. Not only does this utility detect new wireless access points but it will also monitor points that the security manager says are okay. It will also tell you which access points are unsecured and need to be looked at.

Disaster Recovery

Although disaster recovery doesn't deal directly with security, I think that it is important enough to be discussed in this part of the paper. Without a disaster recovery plan, the company would be totally shut down if a disaster happened. Since Giac is a for profit corporation it is very necessary to have a disaster recovery plan and make sure that the backups are running and that you can restore any data that you might need. The following is Giac's backup schedule and disaster recovery plan.

We will be doing full backups weekly on all servers and incremental backups nightly on all servers. The retention period of all data will be two months. This will be done with a product called Legato[5]. This product allows us to backup over the network to a centrally managed tape jukebox system. This also allows us to do restores from the desktop of the machine that needs a file restored. Since we have two sites with a dedicated T3 line in between, we will have a legato server at each site doing backups of all of the servers in the enterprise. This gives us great failover at each site and also allows us to restore the whole corporation if something happens to one site.

One thing that would need to happen if a disaster did happen at one site would be that we would need domain controllers up as soon as possible. With just the Legato system, we would have to reinstall the OS and then restore from backup, delaying the process by several minutes or even hours. To solve this problem we have decided to use a tape drive made by HP. This tape drive uses a technology called HP One-Button Disaster Recovery. We will only use this method on DC01 and will only do it weekly. This allows us to do a full backup of the server on a separate tape. We will ship this tape to the remote site. If anything ever happened to DC01 we could get this tape, put it in the tape drive and boot to the tape it self. The tape will boot up and restore itself to whatever

[4]http:// www.isomair.com
[5]http://www.legato.com

was on the tape. This process takes a total of about thirty minutes. So if something happened to the domain, we could have DC01 back up and running in about 30 minutes.

References

MCSE Windows 2000 Migration Study Guide. San Francisco: Sybex, 2001.

Minasi, Mark. Mastering Windows 2000 Server. San Francisco: Sybex, 1999.

Cox, Philip and Tom Sheldon. Windows 2000 Security Handbook. Berkeley, California: Osborne/McGraw Hill, 2001.

George Spalding. Windows 2000 Administration. Berkeley, California: Osborne/McGraw Hill, 2001.